

Notice of Allowability

Application No.

09/640,606

Examiner

Taghi T. Arani

Applicant(s)

KHANOLKAR ET AL.

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 04/17/2006.
2. ☒ The allowed claim(s) is/are 1-43.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 4/25/2006.
7. ☐ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

Taghi T. Arani,
Primary Examiner
Aug 13 1
Taghi T. Arani
4/25/06

DETAILED ACTION

1. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1, 25, 35 and 36 have been amended.
4. Claims 1-43, now re-numbered as claims 1-43 are pending.

EXAMINER'S AMENDMENT

5. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with George A. Willman on 4/25/2006.

"the user" at the last line of claims 1 and 35 have been replaced with "a user".

Abstract has been replaced with:

ABSTRACT OF THE DISCLOSURE

An embodiment includes a computer system for detecting and monitoring network intrusion events from log data received from network service devices in a computer network. An embodiment may include an event parser in communication with multiple network service devices. The event parser may parse information to create corresponding event objects concerning intrusion events. The system may include an event manager in communication with

Art Unit: 2131

the event parser. The event manager may be configured to evaluate the event objects according to at least one predetermined threshold condition. The system may include an event broadcaster in communication with the event manager for receiving event objects designated by the event manager for broadcast. The event broadcaster may be able to transmit the event objects in real time. The system may also include means for alerting the user that a network intrusion event has occurred.

Response to Arguments

6. Applicant's arguments filed 04/17/2006 in have been fully considered and they are persuasive.

Allowable Subject matter

7. Claims 1-43 are allowed over prior art of record.

Conclusion

8. Prior arts made of record, not relied upon:

US patent 5,805,801 to Holloway et al. is directed to system and method for detecting and preventing security in a campus LAN network.

US 6,119,236 to Shipley teaches intelligent network security device ("INSD") and method in a local area network ("LAN").

US 6,453,345 to Trcka et al. is directed to a network security and surveillance system which passively monitors and records the traffic present on a local area network, wide area network, or other type of computer network.

US 6,553,336 to Johnson et al. teaches smart monitoring system and method.

Art Unit: 2131

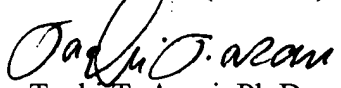
Kelly Jackson Higgins, "SECURITY STRATEGIES—A WELCOME INTRUSION—
Network managers are taking advantage of the move by security companies to pack intrusion
detection into a suite of managed services", InternetWeek. Manhasset: May 29, 2000, Iss. 815;
PG 39.

Scott Blake, Protecting the network neighborhood, Security Management, Arlington:
April 2000, vol. 44, Iss. 4; pg 65, 5 pgs.

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The
examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the
organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent
Application Information Retrieval (PAIR) system. Status information for published applications
may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
applications is available through Private PAIR only. For more information about the PAIR
system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR
system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Taghi T. Arani, Ph.D.
Primary Examiner
Art Unit 2131
4/25/2006